

Des. Codes Cryptogr. (2011) 59:183–191
DOI 10.1007/s10623-010-9454-0

Lower bounds on the size of spheres of permutations under the Chebychev distance

Torleiv Kløve

Received: 10 February 2009 / Revised: 17 April 2009 / Accepted: 1 August 2010 /

Published online: 8 December 2010

© The Author(s) 2010. This article is published with open access at Springerlink.com

Abstract Lower bounds on the number of permutations p of $\{1, 2, \dots, n\}$ satisfying $|p_i - i| \leq d$ for all i are given.

Keywords Permutations · Chebychev distance · Spheres

Mathematics Subject Classification (2000) 05A05 · 94B65

1 Introduction

A class of enumerative combinatorial problems can be formulated as follows. Let S_n denote the set of all permutations of $\{1, \dots, n\}$. Suppose that for each integer $i \geq 1$ we have a set $S[i]$ of positive integers. How many of the permutations p in S_n satisfy $p_i \in S[i]$ for all i , $1 \leq i \leq n$? Problems of this form have been studied for more than a hundred years, and several methods have been developed to attack such problem.

The problem considered in this paper is the enumeration of permutations which satisfy $|p_i - i| \leq d$ for all i . The motivation comes from coding theory. A permutation array is a set of permutations of $[n] = \{1, 2, \dots, n\}$. Recently, Jiang et al. [3, 4] showed an interesting application of permutation arrays to flash memories, where they used different distance metrics to investigate efficient rewriting schemes. In [6], we studied the multi-level flash memory model, using the Chebyshev metric. Another recent paper is [12].

The problem can be rephrased as: what is the size of a sphere of radius d in the set of permutations of length n under the Chebychev distance.

More precisely, we consider the distance d_{\max} between permutations defined by

$$d_{\max}(p, q) = \max_j |p_j - q_j|.$$

T. Kløve (✉)

Department of Informatics, University of Bergen, PO Box 7803, 5020 Bergen, Norway
e-mail: Torleiv.Klove@ii.uib.no

Let ι denote the identity permutation in S_n . The object of study in this paper is $V(d, n)$, the number of permutations in S_n within distance d of the identity permutation, that is

$$V(d, n) = |T_{d,n}|,$$

where

$$T_{d,n} = \{p \in S_n \mid |p_i - i| \leq d \text{ for } 1 \leq i \leq n\}.$$

We note that since $d_{\max}(\iota, q) = d_{\max}(p, pq)$ for any permutation $p \in S_n$, the number of permutations in S_n within distance d of p will also be $V(d, n)$. In [6] this fact was used to obtain a Plotkin type bound for permutation arrays.

In general, no simple expression for $V(d, n)$ is known. As far as I can tell, this particular problem was first discussed by Lagrange [7] in 1962. He limited his study to $d \leq 3$. He found sets of recursions that could be used to compute $V(d, n)$ numerically. The method was ad hoc, and already for $d = 3$, the recursions and the discussion leading up to them became quite complicated. The case $d = 3$ takes over five pages in his paper.

The problem was next considered by Lehmer [8] in 1970. For fixed d , $V(d, n)$ satisfies a linear recurrence in n . Lehmer determined the recurrences and generating functions for $d \leq 3$. The first values of $V(1, n)$, $V(2, n)$, and $V(3, n)$ and the generating functions are given as sequences A000045, A002524, and A002526, respectively, in [10].

One proof of the fact that $V(d, n)$ satisfies a linear recurrence in n is given in Stanley's textbook [11] (Proposition 4.7.8 on page 246); Stanley considers a wider class of related problems and he used a transfer-matrix method.

Baltić studied the problem more recently. Only a very short abstract of his work has been published, in [1], p. 105. He has computed values of $V(4, n)$ for $n \leq 24$, posted in [10] as sequence A072856.

The fact that $V(d, n)$ satisfies a linear recurrence implies that

$$\lim_{n \rightarrow \infty} V(d, n)^{1/n} = \mu_d,$$

where μ_d is the largest root of the polynomial corresponding to the shortest linear recurrence of $V(d, n)$. For $d = 1$, $d = 2$, and $d = 3$, these recurrences were determined explicitly by Lehmer [8] and he also determined μ_d (approximately).

The generating functions for $d \leq 6$, the values of μ_d for $d \leq 8$, and the first 30 values of $V(d, n)$ for $d \leq 10$ are given in [5]. The first values of $V(d, n)$ for $5 \leq d \leq 10$ are posted as sequences A154654–A154659 in [10]. We quote the values of μ_d (and $\mu_d/(2d + 1)$) in the following Table 1.

The purpose of this paper is to study lower bounds on $V(d, n)$.

2 Lower bounds

The permanent of an $n \times n$ matrix A is defined by

$$\text{per } A = \sum_{p \in S_n} a_{1,p_1} \cdots a_{n,p_n}. \quad (1)$$

In particular, if A is a $(0, 1)$ -matrix, then

$$\text{per } A = |\{p \in S_n \mid a_{i,p_i} = 1 \text{ for all } i, 1 \leq i \leq n\}|.$$

Table 1 μ_d , the limit of $V(d, n)^{1/n}$ when n goes to infinity

d	μ_d	$\mu_d/(2d+1)$
1	1.61803	0.53934
2	2.33355	0.46671
3	3.06177	0.43739
4	3.79352	0.42150
5	4.52677	0.41152
6	5.26082	0.40468
7	5.99534	0.39969
8	6.73016	0.39589

Let $A^{(d,n)}$ be the $n \times n$ matrix with $a_{i,j}^{(d,n)} = 1$ if $|i - j| \leq d$ and $a_{i,j}^{(d,n)} = 0$ otherwise. We immediately get the following (well-known) result:

$$V(d, n) = \text{per } A^{(d,n)}.$$

Lehmer [8] stated (without giving any details) that the “van der Waerden conjecture” can be used to prove that

$$\frac{\mu_d}{2d+1} \geq \frac{1}{e} \approx 0.36788. \quad (2)$$

The van der Waerden conjecture (now theorem, see e.g. [13, p.104]) states that for a doubly stochastic $n \times n$ matrix, the permanent is lower bounded by $n!/n^n$. Doubly stochastic means that all the elements are non-negative and that the sum of the elements in any row or column is 1. If A is an $n \times n$ matrix where the sum of the elements in any row or column is k , then van der Waerden’s theorem shows that the permanent is lower bounded by $n!k^n/n^n$.

In $A^{(d,n)}$, most rows and columns have sum $2d+1$, but not all. For a closely related matrix $B^{(d,n)}$, all rows and columns have sum $2d+1$. The matrix $B^{(d,n)}$ is defined as follows:

$$\begin{aligned} b_{i,j} &= 0 && \text{if } i > j + d \text{ or } j > i + d, \\ b_{i,j} &= 2 && \text{if } i + j \leq d + 1 \text{ or } i + j \geq 2n + 1 - d, \\ b_{i,j} &= 1 && \text{otherwise.} \end{aligned}$$

We see that $B^{(d,n)}$ is obtained from $A^{(d,n)}$ by changing elements in the upper left and lower right corners from 1 to 2. From the discussion above we see that

$$\text{per } B^{(d,n)} \geq \frac{n!(2d+1)^n}{n^n} > \sqrt{2\pi n} \left(\frac{2d+1}{e} \right)^n. \quad (3)$$

The elements in $B^{(d,n)}$ with value 2 are all located in the first d and the last d columns. Hence from the definition (1), we see that

$$\text{per } B^{(d,n)} \leq 2^{2d} \text{per } A^{(d,n)}, \quad (4)$$

and so

$$V(d, n) > \frac{\sqrt{2\pi n}}{2^{2d}} \left(\frac{2d+1}{e} \right)^n. \quad (5)$$

We see that (5) implies that

$$(V(d, n))^{1/n} > \left(\frac{\sqrt{2\pi n}}{2^{2d}} \right)^{1/n} \frac{2d+1}{e} \rightarrow \frac{2d+1}{e}$$

when $n \rightarrow \infty$, that is, (2) is true.

One way to improve the lower bound in (5) along the same line is to improve the bound (4), and we (essentially) do this next. Let C be the $d \times 2d$ matrix in the upper left corner of $B^{(d,n)}$, that is, for $1 \leq i \leq d$ we have

$$\begin{aligned} c_{i,j} &= 2 & \text{for } 1 \leq j \leq d+1-i, \\ c_{i,j} &= 1 & \text{for } d+2-i \leq j \leq d+i, \\ c_{i,j} &= 0 & \text{for } d+1+i \leq j \leq 2d. \end{aligned}$$

Further, let

$$\begin{aligned} R_d &= \{(\rho_1, \rho_2, \dots, \rho_d) \mid 1 \leq \rho_i \leq d+i, 1 \leq i \leq d, \text{ and } \rho_r \neq \rho_s \text{ for } r \neq s, \} \\ \sigma(\rho) &= c_{1,\rho_1} c_{2,\rho_2} \cdots c_{d,\rho_d} \quad \text{for } \rho \in R_d, \end{aligned}$$

and

$$\Omega_d = \sum_{\rho \in R_d} \sigma(\rho).$$

For $\rho, \tau \in R_d$, let $\Psi(\rho, \tau, n)$ be the number of permutations $p \in T(d, n)$ such that $p_i = \rho_i$ for $1 \leq i \leq d$ and $p_{n+1-i} = \tau_i$ for $1 \leq i \leq d$. Then

$$\text{per } B^{(d,n+2d)} = \sum_{\rho \in R_d} \sum_{\tau \in R_d} \sigma(\rho) \sigma(\tau) \Psi(\rho, \tau, n+2d).$$

The numbers $\Psi(\rho, \tau, n+2d)$ will vary with ρ and τ . However, we have

$$\Psi(\rho, \tau, n+2d) = \text{per } A_{n,\rho,\tau},$$

where $A_{n,\rho,\tau}$ is the $n \times n$ matrix obtained by removing from $A^{(d,n+2d)}$ the d first and d last rows and the columns ρ_i for $1 \leq i \leq d$ and $n+2d+1-\tau_i$ for $1 \leq i \leq d$. In particular, $A_{n,\rho,\tau}$ is obtained from $A^{(d,n)}$ by changing some ones to zeros (the number of changes is between 0 and $2d$). Hence $\text{per } A_{n,\rho,\tau} \leq V(d, n)$. Therefore

$$\text{per } B^{(d,n+2d)} \leq V(d, n) \sum_{\rho \in R_d} \sigma(\rho) \sum_{\tau \in R_d} \sigma(\tau) = V(d, n) \Omega_d^2.$$

Let

$$\omega_d = \frac{\Omega_d e^d}{(2d+1)^d}.$$

By (3), we get

Theorem 1

$$V(d, n) \geq \frac{\sqrt{2\pi(n+2d)}}{\omega_d^2} \left(\frac{2d+1}{e} \right)^n. \quad (6)$$

This gives an improvement of (5). To show how large the improvement is, we have to determine or at least estimate ω_d . Our argument is heuristic in that one step in the argument will be based on numerical evidence only.

It is not obvious how we can obtain a useful general formula for Ω_d from its definition. We (first) computed Ω_d by exhaustive search for $1 \leq d \leq 7$. In the next table we give these values: :

d	1	2	3	4	5	6	7
Ω_d	3	18	170	2200	36232	725200	17095248

A search in [10] came up with one sequence, A074932, that coincides with these seven first terms. We will denote this sequence by Ω_d^* . A general expression for Ω_d^* is given in [10]:

$$\Omega_d^* = \sum_{m=0}^d \binom{d}{m} (m+1)^d. \quad (7)$$

Since the numbers are so large, it is quite likely that it is not a coincidence that $\Omega_d = \Omega_d^*$ for $d \leq 7$ and that these sequences are the same for all d . We also computed (again by exhaustive search)

$$\Omega_8 = 463936896 \quad \text{and} \quad \Omega_9 = 14246942336$$

and checked that $\Omega_8 = \Omega_8^*$ and $\Omega_9 = \Omega_9^*$ as well. Based on this, we make the following conjecture.

Conjecture 1

$$\Omega_d = \Omega_d^* = \sum_{m=0}^d \binom{d}{m} (m+1)^d \quad \text{for all } d \geq 1. \quad (8)$$

So far, we do not have a proof of this conjecture. However, we will estimate Ω_d^* and get a conjectured estimate for Ω_d . Let

$$\omega_d^* = \frac{\Omega_d^* e^d}{(2d+1)^d}$$

and

$$t_m = \binom{d}{m} \left(\frac{(m+1)e}{2d+1} \right)^d.$$

From (8) we get

$$\omega_d^* = \sum_{m=0}^d t_m. \quad (9)$$

If we write $m = \lambda d$, we have for, $0 < \lambda < 1$ (see e.g. [9, p. 466]):

$$\binom{d}{\lambda d} \approx \frac{1}{\sqrt{2\pi\lambda(1-\lambda)d}} \left(\frac{1}{\lambda^\lambda(1-\lambda)^{1-\lambda}} \right)^d.$$

Let

$$f(\lambda) = \left(\frac{\lambda}{1-\lambda} \right)^{1-\lambda}.$$

Then we get

$$\begin{aligned} t_m &\approx \frac{1}{\sqrt{2\pi\lambda(1-\lambda)d}} \left(\frac{1}{\lambda^\lambda(1-\lambda)^{1-\lambda}} \right)^d \left(\frac{\lambda e}{2} \right)^d \\ &= \frac{1}{\sqrt{2\pi\lambda(1-\lambda)d}} \left(\frac{e}{2} f(\lambda) \right)^d. \end{aligned} \quad (10)$$

The function $f(\lambda)$ is maximal for $\lambda = \lambda_0 \approx 0.78219$, and the maximal value is $\psi = f(\lambda_0) \approx 1.32110$. Hence the maximal t_m is

$$t_{\lambda_0 d} \approx \frac{1}{\sqrt{2\pi\lambda_0(1-\lambda_0)d}} \varphi^d \approx \frac{0.96653}{\sqrt{d}} \varphi^d.$$

where

$$\varphi = \frac{\psi e}{2} \approx 1.79556.$$

Since ω_d^* has $d+1$ terms, clearly,

$$\omega_d^* \lesssim 0.96653 \frac{d+1}{\sqrt{d}} \varphi^d.$$

Numerical computations show that this is a quite weak upper bound. We can show the following much stronger bound:

Lemma 1 *We have*

$$\omega_d^* \lesssim 1.67219 \sqrt{\ln(d) - \ln(\ln(d))} \varphi^d.$$

Proof From the Taylor expansion of $f(\lambda)$ at the point $\lambda = \lambda_0$ we get

$$f(\lambda) = f(\lambda_0) \{1 - \eta(\lambda - \lambda_0)^2\} + O((\lambda - \lambda_0)^3),$$

where

$$\eta = \frac{1}{2\lambda_0^2(1-\lambda_0)} \approx 3.75203.$$

Let

$$\lambda_1 = \lambda_0 - \sqrt{\frac{\ln(\sqrt{d}/\{\ln(d) - \ln(\ln(d))\})}{\eta d}}$$

and

$$\lambda_2 = \lambda_0 + \sqrt{\frac{\ln(\sqrt{d}/\{\ln(d) - \ln(\ln(d))\})}{\eta d}}.$$

From (9) we get

$$\frac{\omega_d^*}{\varphi^d} = S_1 + S_2 + S_3,$$

where

$$S_1 = \sum_{m=0}^{\lfloor \lambda_1 d \rfloor} \frac{t_m}{\varphi^d}, \quad S_2 = \sum_{m=1+\lfloor \lambda_1 d \rfloor}^{\lfloor \lambda_2 d \rfloor} \frac{t_m}{\varphi^d}, \quad S_3 = \sum_{m=1+\lfloor \lambda_2 d \rfloor}^d \frac{t_m}{\varphi^d}.$$

First, we see that

$$\begin{aligned}\ln(\sqrt{d/\{\ln(d) - \ln(\ln(d))\}}) &= \frac{1}{2} \left\{ \ln(d) - \ln(\ln(d)) - \ln\left(1 - \frac{\ln(\ln(d))}{\ln(d)}\right) \right\} \\ &\approx \frac{1}{2} \{\ln(d) - \ln(\ln(d))\}.\end{aligned}$$

Hence,

$$\begin{aligned}S_2 &\lesssim (\lambda_2 - \lambda_1)d t_{\lambda_0 d} \\ &\lesssim 2 \sqrt{\frac{\ln(d) - \ln(\ln(d))}{2\eta}} \cdot 0.96653 \\ &\approx 0.70566 \sqrt{\ln(d) - \ln(\ln(d))}.\end{aligned}$$

For S_1 we get

$$\begin{aligned}S_1 &\lesssim d\lambda_1 \frac{1}{\sqrt{2\pi d\lambda_1(1-\lambda_1)}} \frac{f(\lambda_1)^d}{\psi^d} \\ &\approx \frac{\lambda_1 \sqrt{d}}{\sqrt{2\pi\lambda_1(1-\lambda_1)}} \left(1 - \frac{\ln(\sqrt{d/\{\ln(d) - \ln(\ln(d))\}})}{d}\right)^d \\ &\approx \frac{\lambda_1 \sqrt{d}}{\sqrt{2\pi\lambda_1(1-\lambda_1)}} e^{-\ln(\sqrt{d/\{\ln(d) - \ln(\ln(d))\}})} \\ &= \frac{\lambda_1}{\sqrt{2\pi\lambda_1(1-\lambda_1)}} \sqrt{\ln(d) - \ln(\ln(d))} \\ &\approx \frac{\lambda_0}{\sqrt{2\pi\lambda_0(1-\lambda_0)}} \sqrt{\ln(d) - \ln(\ln(d))} \approx 0.75601 \sqrt{\ln(d) - \ln(\ln(d))}.\end{aligned}$$

Similarly,

$$S_3 \lesssim 0.21052 \sqrt{\ln(d) - \ln(\ln(d))}.$$

From Lemma 1 we see that $\omega_d^* < \sqrt{3(\ln(d) - \ln(\ln(d)))}$ for d sufficiently large, and numerical results strongly indicate that this is the case for all $d \geq 3$. Combining this with (6), we get

$$V(d, n) > \frac{2\sqrt{2}}{3\sqrt{\pi}} \cdot \frac{\sqrt{n+2d}}{\{\ln(d) - \ln(\ln(d))\} 1.79556^{2d}} \left(\frac{2d+1}{e}\right)^n. \quad (11)$$

provided $\Omega_d^* = \Omega_d$. Hence, (6) clearly improves (5) (at least provided $\Omega_d^* = \Omega_d$).

Comments on Conjecture 1

There is an old saying: “If you can’t solve it, generalize it”. The idea is that a more general problem may shed some light on a problem and even lead to a solution. Let us generalize the matrix C to a matrix C_x that has the value x where C has the value 2 and ask the same question as before. To be precise, let C_x be the $d \times 2d$ matrix defined by

$$\begin{aligned}c_{i,j} &= x && \text{for } 1 \leq j \leq d+1-i, \\ c_{i,j} &= 1 && \text{for } d+2-i \leq j \leq d+i, \\ c_{i,j} &= 0 && \text{for } d+1+i \leq j \leq 2d,\end{aligned}$$

and let

$$\Omega_d(x) = \sum_{\rho \in R_d} c_{1,\rho_1} c_{2,\rho_2} \cdots c_{d,\rho_d}. \quad (12)$$

In particular, $\Omega_d(2) = \Omega_d$. A study of (12) gave the following generalization of Conjecture 1; it has been verified for $d \leq 9$.

Conjecture 2

$$\Omega_d(x) = \Omega_d^*(x) = \sum_{m=0}^d \binom{d}{m} (m+1)^d (x-1)^{d-m}.$$

If we expand $(x-1)^{d-m}$, use the relation $\binom{d}{m} \binom{d-m}{j} = \binom{d}{j} \binom{d-j}{m}$, and rearrange the terms we can get the equivalent expression

$$\Omega_d^*(x) = \sum_{j=0}^d x^j \binom{d}{m} \sum_{m=0}^{d-j} \binom{d-j}{m} (m+1)^d (-1)^{d-j-m}.$$

The inner sum can be rewritten using the identity given by Gould [2] in his proof of the Govindarajulu-Suzuki identity. For our parameters this identity can be written:

$$\sum_{m=0}^{d-j} \binom{d-j}{m} (-1)^{d-m} (m-z)^d = \sum_{r=0}^j \binom{d}{d-j+r} (-1)^r (d-j)! z^{j-r} \left\{ \begin{matrix} d-j+r \\ d-j \end{matrix} \right\} \quad (13)$$

for all z . Here, $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ are the Sterling numbers of the second kind. They have a generating function

$$\prod_{k=0}^n (1 - kz)^{-1} = \sum_{k=0}^{\infty} \left\{ \begin{matrix} n \\ k \end{matrix} \right\} z^k.$$

There are several ways of writing the Sterling numbers as finite sums. For actual computations, the recurrence

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} + \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\},$$

with the initial conditions $\left\{ \begin{matrix} n \\ n \end{matrix} \right\} = 1$ for all $n \geq 0$, $\left\{ \begin{matrix} n \\ 0 \end{matrix} \right\} = 0$ for all $n \geq 1$ is often useful.

Letting $z = -1$ in (13), we get

$$\sum_{m=0}^{d-j} \binom{d-j}{m} (-1)^{d-m-j} (m+1)^d = (d-j)! \sum_{r=0}^j \binom{d}{d-j+r} \left\{ \begin{matrix} d-j+r \\ d-j \end{matrix} \right\}.$$

For small j , the right hand side expression is easier to compute, for large j (that is, for small $d-j$), the left hand expression is the easier to compute.

Acknowledgments This research was supported by The Norwegian Research Council.

Open Access This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

References

1. Baltić V.: On the number of certain types of restricted permutations. In: Abstracts of Talks presented at the International Mathematical Conference, Topics in Mathematical Analysis and Graph Theory (MAGT). Univ. Beograd Publ. Elektrotehn. Fak. Ser. Mat. **18**, 93–137 (2007).
2. Gould H.W.: An identity involving Stirling numbers. *Ann. Inst. Stat. Math.* **17**, 265–269 (1965).
3. Jiang A., Mateescu R., Schwartz M., Bruck J.: Rank modulation for flash memories. In: Proceedings of IEEE International Symposium on Information Theory, pp. 1731–1735 (2008).
4. Jiang A., Schwartz M., Bruck J.: Error-correcting codes for rank modulation. In: Proceedings of IEEE International Symposium on Information Theory, pp. 1736–1740 (2008).
5. Kløve T.: Spheres of permutations under the infinity norm—permutations with limited displacement. Report no. 2008-376, Department of Informatics, University of Bergen, Norway. <http://www.iu.uib.no/publikasjoner/texrap/pdf/2008-376.pdf>.
6. Kløve T., Lin T.-T., Tsai S.-C., Tzeng W.-G.: Permutation arrays under the Chebyshev distance. *IEEE Trans. Inform. Theory* **56**(6), 2611–2617 (2010).
7. Lagrange R.: Quelques résultats dans la métrique des permutations. *Annales Scientifiques de l'École Normale Supérieure* **79**, 199–241 (1962).
8. Lehmer D.H.: Permutations with strongly restricted displacements. In: Erdős P., Rényi A., Sós V.T. (eds.) *Combinatorial Theory and its Applications II*. North Holland Publication, Amsterdam, pp. 755–770 (1970).
9. Peterson W.W., Weldon E.J.: *Error-Correcting Codes*. MIT Press, Cambridge (1972).
10. Sloane N.J.A.: The On-Line Encyclopedia of Integer Sequences. <http://www.research.att.com/~njas/sequences/>.
11. Stanley R.P.: *Enumerative Combinatorics*, vol. I. Cambridge University Press, Cambridge (1997).
12. Tamo I., Schwartz M.: Correcting Limited-Magnitude Errors in the Rank-Modulation Scheme. *IEEE Trans. Inform. Theory* **56**(6), 2551–2560 (2010).
13. van Lint, J.H., Wilson, R.M.: *A Course in Combinatorics*, 2nd edn. Cambridge University Press, Cambridge (2001).